1 Erasure Warm-Up

Working over GF\((q)\), you want to send your friend a message of \(n = 4\) packets and guard against 2 lost packets. What is the minimum \(q\) you can use? What is the maximum degree of the unique polynomial that describes your message?

2 Lagrange Interpolation

Find a unique real polynomial \(p(x)\) of degree at most 3 that passes through points \((-1, 3), (0, 1), (1, 2),\) and \((2, 0)\) using Lagrange interpolation.

(a) Find \(\Delta_{-1}(x)\) where \(\Delta_{-1}(0) = \Delta_{-1}(1) = \Delta_{-1}(2) = 0\) and \(\Delta_{-1}(-1) = 1\).

(b) Find \(\Delta_0(x)\) where \(\Delta_0(-1) = \Delta_0(1) = \Delta_0(2) = 0\) and \(\Delta_0(0) = 1\).

(c) Find \(\Delta_1(x)\) where \(\Delta_1(-1) = \Delta_1(0) = \Delta_1(2) = 0\) and \(\Delta_1(1) = 1\).

(d) Find \(\Delta_2(x)\) where \(\Delta_2(-1) = \Delta_2(0) = \Delta_2(1) = 0\) and \(\Delta_2(2) = 1\).

(e) Reconstruct \(p(x)\) by using a linear combination of \(\Delta_{-1}(x), \Delta_0(x), \Delta_1(x),\) and \(\Delta_2(x)\).

3 Where Are My Packets?

Alice wants to send the message \((a_0, a_1, a_2)\) to Bob, where each \(a_i \in \{0, 1, 2, 3, 4\}\). She encodes it as a polynomial \(P\) of degree \(\leq 2\) over GF\((5)\) such that \(P(0) = a_0, P(1) = a_1,\) and \(P(2) = a_2,\) and she sends the packets \((0, P(0)), (1, P(1)), (2, P(2)), (3, P(3)), (4, P(4))\). Two packets are dropped, and Bob only learns that \(P(0) = 4, P(3) = 1,\) and \(P(4) = 2\). Help Bob recover Alice’s message.

(a) Find the multiplicative inverses of 1, 2, 3, and 4 modulo 5.

(b) Find the original polynomial \(P\) by using Lagrange interpolation or by solving a system of linear equations.

(c) Recover Alice’s original message.
4 Secrets in the United Nations

The United Nations (for the purposes of this question) consists of \( n \) countries, each having \( k \) representatives. A vault in the United Nations can be opened with a secret combination \( s \). The vault should only be opened in one of two situations. First, it can be opened if all \( n \) countries in the UN help. Second, it can be opened if at least \( m \) countries get together with the Secretary General of the UN.

(a) Propose a scheme that gives private information to the Secretary General and \( n \) countries so that \( s \) can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: in order for a country to help, all of the country’s \( k \) representatives must agree. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary General and to each representative of each country.